An Optimal Symmetric Secret Distribution of Star Networks[1]

Bruhadeshwar Bezawada
Department of Computer Science
International Institute of
Information Technology
Hyderabad, India 500032

Sandeep S. Kulkarni
Department of Computer Science
and Engineering
Michigan State University
East Lansing MI 48824, USA

Abstract

In this paper, we present a lower bound on secret distribution in star network. Examples of star communication network exist in various systems including sensor networks where there is one base station and several sensors that need to communicate with it. While the previous result had shown the possibility of performing secret distribution in a star network using $2 \log n$ secrets, the lower bound for this problem was unknown. With this motivation, in this paper, we derive a tight bound for the number of secrets required for secret distribution in a star network. We show that as n, the number of *satellite* nodes in the star network, tends to ∞, it suffices to maintain $\log n + 1/2 \log \log n + 1$ secrets at the center node. However, $\log n + 1/2 \log \log n$ secrets do not. Even in the absence of the constraint of $n \to \infty$, we argue that these bounds are reasonably tight, i.e., there are several examples for finite values of n where $\lceil \log n + 1/2 \log \log n \rceil$ secrets do not suffice although $\lceil \log n + 1/2 \log \log n + 1 \rceil$ secrets suffice for virtually all cases of practical interest. We also show that our protocol could provide a tradeoff between internal and external attacks and to reduce the number of secrets in acyclic, planar and fully connected bipartite graphs.

[1] Email: bezawada@iiit.ac.in, sandeep@cse.msu.edu
Web: `http://www.cse.msu.edu/~sandeep`.

This work was partially sponsored by NSF CAREER CCR-0092724, DARPA Grant OSURS01-C-1901, ONR Grant N00014-01-1-0744, NSF grant EIA-0130724, and a grant from Michigan State University.

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE **An Optimal Symmetric Secret Distribution of Star Networks**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Michigan State University,Department of Computer Science and Engineering,East Lansing,MI,48824**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In this paper, we present a lower bound on secret distribution in star network. Examples of star communication network exist in various systems including sensor networks where there is one base station and several sensors that need to communicate with it. While the previous result had shown the possibility of performing secret distribution in a star network using 2 log n secrets, the lower bound for this problem was unknown. With this motivation, in this paper, we derive a tight bound for the number of secrets required for secret distribution in a star network. We show that as n, the number of satellite nodes in the star network, tends to 1, it suffices to maintain log n + 1/2 log log n + 1 secrets at the center node. However, log n + 1/2 log log n secrets do not. Even in the absence of the constraint of n ! 1, we argue that these bounds are reasonably tight, i.e., there are several examples for finite values of n where dlog n+1/2 log log ne secrets do not suffice although dlog n + 1/2 log log n + 1e secrets suffice for virtually all cases of practical interest. We also show that our protocol could provide a tradeoff between internal and external attacks and to reduce the number of secrets in acyclic, planar and fully connected bipartite graphs.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**13**	

1 Introduction

Consider the problem of secure communication in an undirected graph G(V, E), where V is the set of nodes and E is the set of edges. An edge of the form (v_1, v_2), $v_1, v_2 \in V$, specifies that node v_1 *needs* to communicate securely with node v_2. Note that whether the nodes *need* to communicate with each other is orthogonal to whether they *can* communicate with each other directly. In particular, the former is based on application semantics whereas the latter is based on communication characteristic. For example, in a sensor network, a sensor may *need* to communicate securely with a base station. This communication may itself be assisted by other sensors in terms of routing. However, the intermediate sensors can neither learn the contents of the message nor can generate messages on behalf of the sender.

Our problem in this paper is motivated by the above scenario where the communication graph is a star, i.e., it consists of one center node and several satellite nodes. The center node uses unicast or broadcast to communicate with the satellite nodes and the satellite nodes use unicast to communicate with the center node. No two satellite nodes need to communicate with each other. All the communication between the center node and the satellite nodes needs to be authenticated. By authentication we mean that, any impersonation attempt by the satellite nodes or outside nodes is prevented.

Our approach for authentication is as follows: Each node (center and satellite) has a set of secrets. Whenever a node sends a message, it adds authentication codes based on some of the secrets it has. Upon reception, the receiver verifies some of the authentication codes that it receives. It is required that message must be authentic when the receiver verifies the required authentication codes.

With this motivation, we focus on secret distribution that will provide authentication for the communication in star networks. In our work, we focus on the secrets that should be given to each node; it does not address how these secrets are distributed. In case of sensor networks, these secrets can be distributed at deployment time. Or, they could be communicated using other approaches such as the use of public keys etc.

We first precisely define the problem of communication in star network. In particular, we identify constraints on the broadcast communication from the center node to satellite nodes. Essentially, these constraints require that the *cost* of the broadcast communication should be proportional to the secrets that the center node maintains. Then, we present our approach for secret distribution and its optimality.

The main results in this paper are as follows:

- We show that as the number of satellite nodes in the star network, say n, tends to ∞
  - There exists a protocol that maintains $\log n + 1/2 \log\log n + 1$ secrets at the center node.

  - Under the assumption that the number of secrets maintained by the satellite nodes is identical, we show that there does not exist a protocol that maintains $\log n + 1/2 \log\log n$ secrets at the center node.

- In the absence of the constraint of $n \rightarrow \infty$, we show that

  - There exists a protocol (shown constructively) that maintains $\lceil \log n + 1/2 \log\log n + 1 \rceil$ secrets at the center node for virtually all cases of practical interest.
  - Under the assumption that the number of secrets maintained by the satellite nodes is identical, there does not exist a protocol that maintains $\lceil \log n + 1/2 \log\log n \rceil$ secrets at the center node for many cases of practical interest.

- We show that our protocol can also be extended to acyclic, limited cycle and fully connected bipartite networks.

- We show that our protocol provides tradeoff between internal attackers and external attackers.

Organization of the paper. The rest of the paper is organized as follows. In section 2, we precisely define the problem of secret distribution. In section 3, we provide our algorithm for secret distribution in a star network and show its optimality. In Section 4, we show how our solution can be extended to acyclic, planar and fully connected bipartite graphs. In Section 5, we show how our solution provides a tradeoff between internal and external attacks. Finally, in section 6, we discuss related work and conclude in Section 7.

2 Constraints on Communication in Star Network and Problem Statement

In this section, we identify the constraints on the broadcast communication from the center node to the satellite nodes. To motivate these constraints, consider the following solution:

In this solution, the center node maintains a secret x. Each satellite node has an ID ranging from $1 \ldots n$. The secret associated with satellite node j is $f(x, j)$. Clearly, $f(x, j)$ could be used for unicast communication to/from j and the center node. (For example, $f(x, j)$ could be used to generate a message digest that the receiver can verify. Since $f(x, j)$ is known only to the center node and satellite node j, only they can generate the corresponding message digest.) However, for broadcast, the center node must provide authentication code using $f(x, j)$, $1 \leq j \leq n$. Each satellite node can verify the authentication code by generating the code locally, using its secret $f(x, j)$, and comparing the generated code with the code sent by the center node.

Clearly, in the above solution, the cost of generating authentication codes, which is $O(n)$, for broadcast is very high. Motivated by this undesirable solution, we impose the following constraint on the problem of secret distribution in star network: We require that the center node maintain a set of secrets, say of size k. Each satellite node maintains a unique subset of these secrets. Whenever the center node sends a broadcast message, it provides authentication codes using some/all of those secrets. For example, if the center node broadcasts the message to a subset of the satellite nodes, say, $i_1, \ldots, i_t$, then the center node generates authentication codes using the secrets that are in the union of all the subsets of secrets held by these satellite nodes. Since the authentication codes are generated using the secrets held by target satellite nodes, those nodes can verify the authenticity of the message. For broadcast messages sent to all the satellite nodes, the center uses the same technique and hence, generates authentication codes using all k secrets.

Note that the earlier solution also fits in this category if we consider that the secrets maintained at the center node are $f(x, j)$, $1 \leq j \leq n$. However, this representation clearly captures that the number of secrets maintained at the center node is n and each satellite node maintains one secret from these secrets.

Based on the above discussion, the problem statement for secret distribution in a star network is as follows: The center node maintains a set of secrets, say of size k. Each satellite node maintains a subset, say of size l, of this set of secrets. To broadcast a message, the center node provides authentication codes based on all k secrets. The satellite node verifies the l authentication codes that it can verify. The problem is to reduce the size of the set of secrets at the center node while allowing it to send unicast, multicast, and broadcast messages in an authenticated manner.[2] Note that, it is required that the satellite node must be able to derive authenticity of a message by verifying the required authentication codes.

3 Authenticated Communication in Star Network and its Optimality

As discussed in the previous section, in our protocol, the center node maintains a set of k secrets. Each satellite node receives a unique subset of size l from this set. Note that, by construction, no two satellite nodes have identical subsets of secrets. Similar to [1], we use this secret distribution protocol to achieve secure and authenticated communication. We term this protocol instance as $p(k, l)$ [3]. Using $p(k, l)$, authentication can be achieved in the communication as follows:

[2] The problem of reducing the secrets at the satellite node is not considered, since this number can be reduced to 1 using the solution considered above.

[3] Technically, $p(k, l)$ is a family of protocols. However, for brevity of presentation, we denote $p(k, l)$ as a protocol. However, we note that all the results in this paper attributed to *protocol* $p(k, l)$ are valid for any member of the $p(k, l)$ protocol family

- To authenticate a message m broadcasted by the center node to the satellite node, the center node generates authentication codes with each of the k secrets. Each authentication code consists of the message digest md of the message computed using a secret held by the center. The center appends the k authentication codes thus generated to the message and broadcasts the resulting message. Now, when a satellite node receives this message, it uses its subset of l secrets to compute l authentication codes. The satellite node then verifies these authentication codes with the corresponding authentication codes sent by the satellite node. Note that, each satellite node can verify only those authentication codes for which it has the corresponding generating secret.

- To authenticate a unicast message m from the center to a particular satellite node, the center node first computes an XOR of the subset of the keys that this satellite node knows. Now, the center node uses the combined secret to compute the message authentication code for this message. The center node appends this authentication code to the message and unicasts the message to the satellite node.

- To authenticate a unicast message m from a satellite node to the center, the satellite node uses the same approach used by the center node for authenticating unicast messages.

In the remaining section, we consider the case where the number of satellite nodes, n, tends to ∞: First, we show (cf. Theorem 4) that $\log n + \log\log n$ secrets suffice at the center to handle n users. Then, we show (cf. Theorem 5) that $\log n + c \log\log n$ secrets do not suffice if $c < 1/2$. Using the proofs of these results, we show (cf. Theorem 6) that $\log n + 1/2 \log\log n + 1$ secrets suffice to handle n nodes whereas $\log n + 1/2 \log\log n$ do not.

Theorem 1. $p(k, l)$ provides authentication for the communication in the star network.

Proof. The proof follows from the construction of $p(k, l)$. □

Theorem 2. Protocol $p(k, l)$ can accommodate upto $C(k, l)$ satellite nodes.

Proof. This follows directly, as this $C(k, l)$ is the number of unique subsets of keys that can be generated. □

Corollary 3. For a given value of k, choosing $l = k/2$ maximizes the number of satellite nodes that can be accommodated. □

Theorem 4. As $n \to \infty$, protocol $p(k, l)$, where $k = \log n + \log\log n$ and $l = k/2$, provides authentication for the star network with n nodes.

Proof. To prove this, we show that, when $k = \log n + \log\log n$ and $l = k/2$, [4] the number of unique subsets of secrets that are possible i.e., $C(k, l) \geq n$. This implies that

[4] Since we are dealing with large values of n, for simplicity of presentation, we omit the floor/ceiling operations required in computing $\log n$, l, etc.

each satellite node receives a different subset of secrets and hence, based on Theorems 1 and 2, $p(k, l)$ can be used for authentication in star network.

We use Stirling's approximation for factorials which states that, for large values of n, $n! \approx (n/e)^n.\sqrt{2\pi n}$. Now, $C(k, l) {=} \frac{k!}{(l)!(k-l)!}$. Since $l = k/2$, this values simplifies to: $\frac{k!}{(k/2)!(k/2)!}$. Now, using Stirling's approximation, we have

$$\begin{aligned} C(k, k/2) &= \frac{k!}{(k/2)!(k/2)!} \\ &\approx \frac{(k/e)^k * \sqrt{2\pi k}}{((k/2e)^{k/2} * \sqrt{2\pi(k/2)})^2} \\ &= \frac{2^k * 2}{\sqrt{2\pi k}} \end{aligned}$$

$\{$Now, letting $k = (\log n + \log\log n)$ $\}$

$$\begin{aligned} &= \frac{2^{(\log n + \log\log n)} * 2}{\sqrt{2\pi(\log n + \log\log n)}} \\ &= n\frac{2\log n}{\sqrt{2\pi(\log n + \log\log n)}} \end{aligned}$$

Now, as $n \to \infty$, the multiple of n tends to ∞. Hence, as $n \to \infty$, $C(k, k/2) > n$, where $k = \log n + \log\log n$. In other words, the number of subsets generated by choosing $k = \log n + \log\log n$ and $l = k/2$ is greater than or equal to n. Thus, this secret distribution ensures authentication in the star network. □

When compared to the secret distribution for star network in [1] our secret distribution requires lesser number of secrets. In [1], the center maintains $2\log n$ secrets and in our secret distribution protocol the center only needs to maintain $\log n + O(\log\log n)$ secrets. The number of secrets stored by the satellite nodes is reduced as well. In [1], each satellite node maintain $\log n$ secrets and in our secret distribution protocol, each satellite node maintains atmost $(\log n)/2 + O(\log\log n)$ secrets. This value represents the upper bound for the number of secrets maintained by the satellite node. Moreover, the result from the above theorem can be verified for most small values of n. In particular, we have verified that $\lceil \log n + \log\log n \rceil$ secrets suffice for $5 < n < 1000$ nodes.

Next, we consider whether the number of secrets can be reduced further. It turns out that not significant reduction can be achieved, as shown in the next theorem.

Theorem 5. As $n \to \infty$, protocol $p(k, l)$ where $k = (\log n + c\log\log n)$, where $c < 1/2$ and $l = k/2$ cannot provide authentication for the star network with n nodes.

Proof. As before we evaluate $C(k,l)$ using Stirling's approximation and show that this value is less than n. Based on Theorems 1 and 2, this result proves this theorem. From the above proof,

$C(k,k/2) \approx \frac{2^k*2}{\sqrt{2\pi k}}$

$\{$Now, letting $k = \log n + c\log\log n\}$

$$= \frac{2^{(\log n + c\log\log n)}*2}{\sqrt{2\pi(\log n + c\log\log n)}}$$

$$= n\frac{2*2^{c\log\log n}}{\sqrt{2\pi(\log n + c\log\log n)}}$$

$$= n\frac{2*(2^{\log\log n})^c}{\sqrt{2\pi(\log n + c\log\log n)}}$$

$$= n\frac{2*(\log n)^c}{\sqrt{2\pi(\log n + c\log\log n)}}$$

Note that, as $n \to \infty$, the multiple of n in the above formula tends to 0. Hence, as $n \to \infty$, $C(k,k/2) < n$. □.

Based on the above theorem, if $c = 1/2$ then the multiple of n is $\frac{2}{\sqrt{2\pi}}$. Since this number of less than 1, $\log n + c\log\log n$ secrets do not suffice when $c = 1/2$. However, if the number of secrets is $(\log n + 1/2\log\log n + 1)$, then in the above formula, the multiple of n is $\frac{4}{\sqrt{2\pi}}$. Since this number is greater than 1, $(\log n + 1/2\log\log n + 1)$ secrets suffice for key distribution in a star network as $n \to \infty$. Thus, we have

Theorem 6. As $n \to \infty$, protocol $p(k,l)$ where $k = (\log n + 1/2\log\log n)$, and $l = k/2$ cannot provide authentication for the star network with n nodes. And, as $n \to \infty$, protocol $p(k,l)$ where $k = (\log n + 1/2\log\log n + 1)$, and $l = k/2$ can provide authentication for the star network with n nodes. □

Once again, since the above theorem applies for the case where $n \to \infty$, the natural question is about what happens for small values of n. Here, we note that we checked whether $\lceil \log n + 1/2\log\log n \rceil$ secrets suffice for $n < 50000$. For $2 \leq n \leq 1000$, we found this number to be insufficient for 510 values and for $1000 \leq n \leq 50000$, we found that this number to be insufficient for 20313 values. By contrast, if we consider $\lceil \log n + 1/2\log\log n + 1 \rceil$ secrets then this number suffices for the case where the number of nodes is less than 50000. As an illustration, we refer the reader to Figure 1.

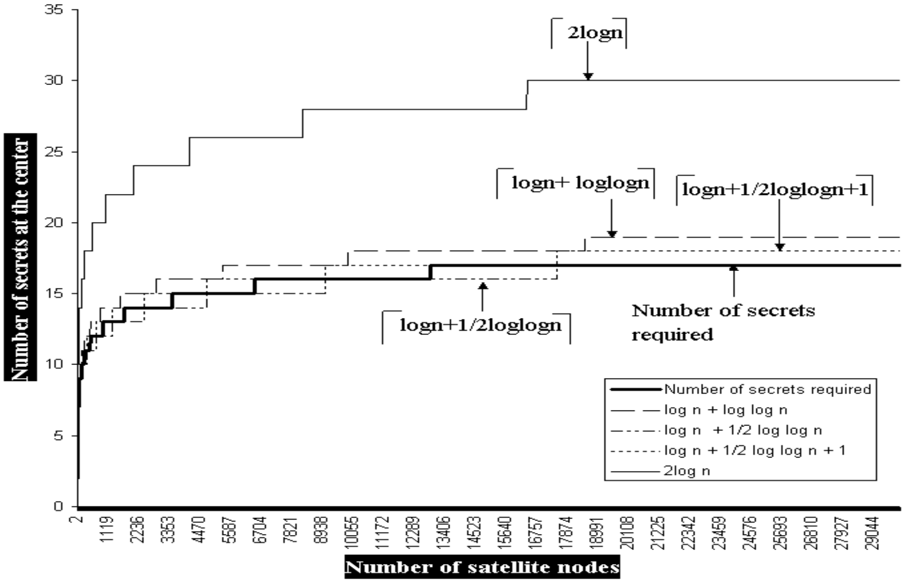

Figure 1: Number of secrets stored by the center node

3.1 Optimality of Secret Distribution in Star Networks

Consider the problem of secret distribution in star network where the number of secrets stored by the satellite nodes is equal. Thus, based on the constraints in Section 2, a solution is of the form where, for some values of k and l, the center node maintains k secrets and each satellite node maintains a subset of size l from that set. In other words, a solution is of the form $p(k, l)$ for some value of k and l. Now, based on Theorem 6, as $n \rightarrow \infty$, $\log n + 1/2 \log \log n + 1$ is the minimum number of secrets that need to be maintained by the center node.

We would like to note that while the reduction in the number of secrets is from $2 \log n$ to $\log n + O(\log \log n)$, this reduction is especially valuable when we consider the number of nodes that can be supported with a given set of secrets at the center. For example, Figure 2 compares the number of nodes that can be supported with our scheme with that in [1]. If 10 secrets are available at the center then the scheme in [1] can support upto 32 satellite nodes whereas our protocol can tolerate upto 252 satellite nodes. Or, if 20 secrets are available at the center then the scheme in [1] can support upto 1024 satellite nodes whereas our protocol can tolerate upto 184756 satellite nodes.

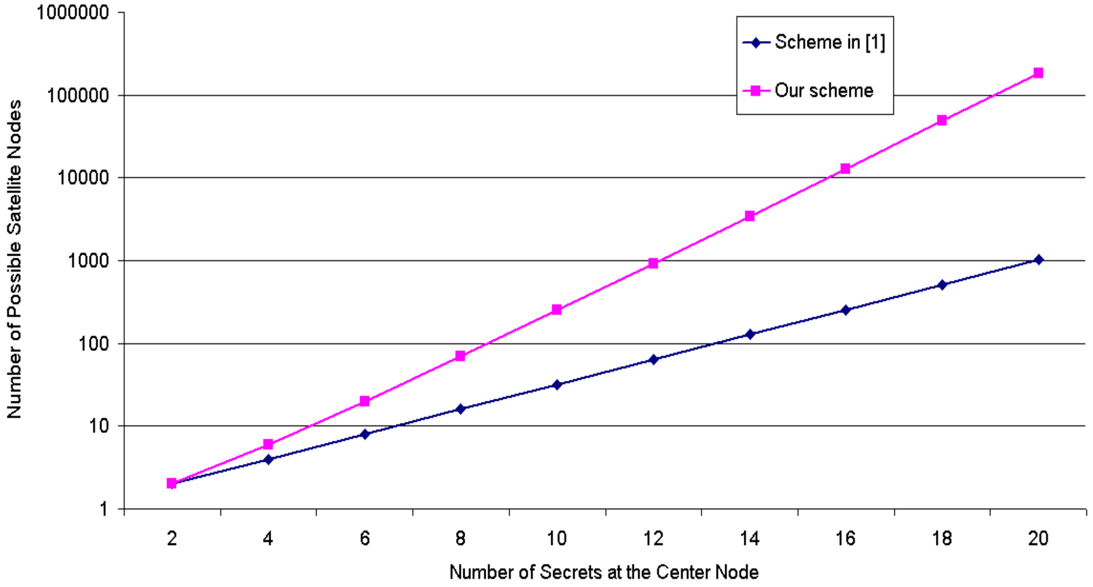

Figure 2: Number of users supported by the center node

4 Extensions to Acyclic, Planar and Complete Bipartite Networks

In Section 3, we described our secret distribution protocol, $p(k,l)$, for a star network. In this section, we extend it for the cases where the communication graph is acyclic, planar, or complete bipartite.

Acyclic Networks. Since an acyclic undirected graph consists of a set of trees, we describe the secret distribution for a tree. The same algorithm can be applied for each tree separately to obtain the secret distribution for acyclic graphs. Given a tree, we choose one of the nodes in it as a root and consider the corresponding rooted version. In particular, this allows us to define a parent of node in the tree and to define whether a node is a leaf. Now, consider a non-leaf node and its children in this network. This sub-network is a star graph where the non-leaf node is the center node and the children are satellite nodes. Now, we apply the $p(k,l)$ secret distribution with appropriate values of k and l for this star graph. We repeat this process for each star graph obtained by considering a non-leaf node and its children. The secrets assigned to a node in the tree are the same as the union of the secrets assigned to it in any star graph considered in this fashion.

Now, in the star graph, the non-leaf node which is the center node gets $\log d + O(\log\log d)$ secrets and each satellite node gets $1/2 \log d + O(\log\log d)$ secrets, where d is the degree of the center node. Furthermore, for any given non-leaf node, it is a center node in at most one star graph considered above. Likewise, it is a satellite node in at most one star graph (where its parent is the center node) considered above. Thus, the number of secrets at any node is at most $3/2 \log d + O(\log\log d)$, which is less than that in [1] where $2 \log d$ secrets are maintained.

Planar Networks. The extension to planar network is similar to that in [1]. In particular, in [1], a well-known result from graph theory (e.g., [2]) is used for extension to planar graphs. The result in [2] states that any planar graph G can be decomposed into at most three acyclic graphs, called $factors$. Each factor has the same nodes as the original graph G and the degree of each factor is at most the degree of the original graph. Now, secrets can be independently distributed to each factor to obtain the secret distribution of planar network. By using our scheme for acyclic networks, it would be possible to reduce the number of secrets used in planar networks as well.

Fully Connected Bipartite Graphs. A complete bipartite graph is a graph $G(V, E)$ such that its vertex set can be partitioned into two disjoint sets, V_1 and V_2, the edge set, E is induced by these two vertex sets such that every vertex in V_1 is connected to every other vertex in V_2. No edge exists between any of the vertices in V_1 (respectively, V_2). Examples of such communication graph is one where the vertex set V_1 contains servers and the vertex set V_2 contains clients. The communication is from servers to clients and vice-versa. No server (respectively, client) needs to communicate with each other.

For this network, we employ the following secret distribution technique. We treat the vertex set V_1 as a single center node, say C, and the vertex set V_2 as satellite nodes. As this represents a star network with C as star node, we instantiate a $p(k, l)$ secret distribution for this network. Thus, in this distribution, the node C needs to store $\log |V_2| + O(\log\log |V_2|)$ secrets. Since C represents the vertex set V_1, each of the nodes in V_1 are given all these secrets. We repeat this procedure by treating the vertex set V_2 as the center node and the vertex set V_1 as the satellite nodes. This secret distribution would provide an additional $1/2 \log |V_1| + O(\log\log |V_1|)$ secrets to each node in V_1. Thus, the number of secrets given to nodes in V_1 is $3/2 \log d + O(\log\log d)$, where $d = max(|V_1|, |V_2|)$ is the maximum degree of any node in the communication graph.

5 Tradeoff in Handling Internal and External Attacks

In this section, we show that our secret distribution protocol can provide a tradeoff between handling internal vs external attacks. An internal attack is launched by two or more colluding satellite nodes that are currently part of the network. These satellite nodes combine their secrets and try to compromise all the secrets of the center node. The goal of an internal attack is to impersonate the center node and inject false information into the network or tamper the messages sent by the center node. Note that, in the protocol in [1], two specifically chosen users are sufficient to compromise all the center node secrets.

An external attack is launched by an intruder who is not part of the network but is able to listen on to the communication in the network. The goal of the external attacker is to impersonate one of the nodes in the network, i.e., it wants to send a message (and the corresponding authentication codes) to the center node and have it accepted as a genuine message. (Note that we are not concerned with replay of genuine packets, as it can be handled using standard techniques.)

To illustrate the tradeoff between internal and external attacks, consider two protocols $p(k, l)$, where $l = k/3$ or $l = 2k/3$. (For simplicity assume that k is a multiple of 3.) Since $C(k, k/3) = C(k, 2k/3)$, the number of nodes that can be handled in either protocols is same. Now, consider the effect of these protocol instances on the two types of attacks.

- For $p(k, k/3)$, the number of secrets held by a satellite node is small. In this case, at least three internal attackers must collude to collect all the center secrets. By contrast, for $p(k, 2k/3)$, the number of secrets held by a satellite node is large. And, only two internal attackers can collude to collect all the center secrets.
- For $p(k, k/3)$, an external attacker only needs to generate $k/3$ valid authentication codes whereas for $p(k, 2k/3)$, an external attacker needs to generate $2k/3$ valid authentication codes. This issue needs to be considered especially if weak authentication codes are used due to resource constraints, e.g., when only a small number of bytes generated by a hash function are included.

The above discussion shows that our secret distribution protocol provides tradeoffs for handling internal and external attacks. Although we have illustrated these tradeoffs with $p(k, k/3)$ and $p(k, 2k/3)$, these tradeoffs can be generalized as $p(k, k/c)$ and $p(k, k(1-1/c))$ where $c > 1$. Depending on the nature of the attacks or the storage capabilities of the satellite nodes, the value of c can be appropriately chosen to achieve the desired secret distribution.

6 Related Work

Secure communication among a group of nodes in a communication network using symmetric key mechanisms has been widely studied. In particular, it has been shown by [3, 4], that the number of secrets stored by each node can be less than $O(n)$ for a system of n nodes. In [3, 4], the authors describe a secret distribution protocol which allow any two users to communicate securely while storing only $O(\sqrt{n})$ secrets. These protocols, are designed for the case where the communication graph is fully connected.

In [5], the authors improve upon this storage requirement and describe a secret distribution protocol that requires each user to store $O(\log^2 n)$ secrets. In their work, the authors show the existence of $O(\log n)$ secret distribution protocol for star network like scenarios for a communication network without actually constructing the protocol. Reducing the storage to logarithmic bounds has benefits in resource constrained networks such as sensor networks. In a sensor network each node has limited memory for storing secrets. Examples of such resource constrained networks include sensor networks [6, 7], ad-hoc networks [8–10] and mobile networks [11, 12].

In [1], the authors describe a logarithmic secret distribution protocol for a star network where the storage is logarithmic for both the center, which stores $2 \log n$ secrets and the satellite nodes, which store $\log n$ secrets. They extend their results to achieve logarithmic secret distribution for several classes of communication networks including, star networks, acyclic networks, cycle-limited networks, planar networks and dense bipartite networks.

7 Conclusion

In this paper, we presented a lower bound on secret distribution in star network. We showed that this lower bound is indeed achievable and tight. In particular, we showed that as $n \to \infty$, $\log n + 1/2 \log \log n + 1$ secrets at the center node suffice. However, $\log n + 1/2 \log \log n$ secrets do not. Even in the absence of the constraint of $n \to \infty$, we find that these bounds are reasonably tight, i.e., there are several examples for finite values of n where $\lceil \log n + 1/2 \log \log n \rceil$ secrets do not suffice although $\lceil \log n + 1/2 \log \log n + 1 \rceil$ secrets suffice for virtually all cases of practical interest. We also showed that our protocol could provide a tradeoff between internal and external attacks.

The result in this paper reduces the number of secrets to almost half compared to that in [1] where $2 \log n$ secrets are used at the center node and $\log n$ secrets are used at the satellite nodes. By contrast, our protocol uses $1/2 \log n + O(\log \log n)$ secrets at satellite nodes.

Using this protocol, we showed that it is possible to reduce the secrets maintained in an acyclic, planar and fully bipartite communication graph. However, the optimality of the number of secrets in these protocols is still an open question. Also, in [1], authors have presented how their approach can be used in limited-cycle graphs and arbitrary bipartite graphs. However, since this extension is based on a specific numbering scheme, it cannot be directly applied with protocol $p(k, l)$. One of the future work in this area is to identify lower bounds for secrets in such graphs.

References

[1] Gouda M. G., Kulkarni S. S., and Elmallah S. E. Logarithmic keying of communication networks. In *8th International Symposium on Stabilization, Safety, and Security of Distributed Systems, SSS-06*, 2006.

[2] Colbourn C. J. *The Combinatorics of Network Reliability.* Oxford University Press, 1987.

[3] Li Gong and David J. Wheeler. A matrix key-distribution scheme. *Journal of Cryptology*, 2(1):51–59, 1990.

[4] Kulkarni S. S., Gouda M. G., and Arora A. Secret instantiation in ad-hoc networks. *Computer Comunications*, (29):200–215, 2006.

[5] Aiyer A.S., Alvisi L, and Gouda M. G. Key grids: A protocol family for assigning symmetric keys. In *IEEE International Conference on Network Protocols*, 2006.

[6] Eschenauer L and Gligor V. D. A key-management scheme for distributed sensor networks. In *9th ACM Conference on Computer and Communications Security*, pages 41–47, New York, NY, USA, 2002. ACM Press.

[7] Perrig A., Szewczyk R., Tygar J. D., Wen V., and Culler D.E. Spins: security protocols for sensor networks. *Wireless Networks*, 8(5):521–534, 2002.

[8] Hubaux J.P Buttyan K and Capkun S. The quest for security in mobile ad hoc networks. In *Mobihoc '01: Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 146–155, New York, NY, USA, 2001. ACM Press.

[9] Yang H., Luo H., Ye F., Lu S., and Zhang L. Security in mobile ad hoc networks: challenges and solutions. *IEEE Wireless Communications*, (11):38–47, 2004.

[10] Bezawada Bruhadeshwar and Sandeep S. Kulkarni. User revocation in secure adhoc networks. In *ICDCIT*, pages 377–388, 2005.

[11] Tatebayashi M., Matsuzaki N., and Newman D. Key distribution protocol for digital mobile communication-systems. *Lecture Notes in Computer Science: Advances in Cryptology*, (435):324–333, 1989.

[12] Mu Y. and Varadharajan V. On the design of security protocols for mobile communications. *Lecture Notes in Computer Science: Information Security and Privacy*, 1172:134–145, 1996.